



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,192	08/30/2001	Hideaki Watanabe	09792909-5126	1206

26263 7590 03/24/2005

SONNENSCHN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER

ELMORE, JOHN E

ART UNIT PAPER NUMBER

2134

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/944,192

Applicant(s)

WATANABE ET AL.

Examiner

John Elmore

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 August 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-40 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-40 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-40 have been examined.

Objections to Specification

2. **Claim 1 is objected to** because of the following informalities: the term "temperature" (line 7) should read "template". Appropriate correction is required.
3. **Claims 6 and 16 are objected to** because of the following informalities: the term "makes a deal with" (line 3) should read "provides services to". Appropriate correction is required.
4. **Claims 8, 17 and 33 are objected to** because of the following informalities: the term "makes a deal with" (line 3) should read "provides services to" and the term "making a deal with" (line 5) should read "providing services to". Appropriate correction is required.
5. **Claims 10 and 20 are objected to** because of the following informalities: the term "any one of" (line 2) should be followed by a colon (i.e. "any one of:"). Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. **Claims 10, 15-20 and 32-35 are rejected under 35 U.S.C. 112, second paragraph**, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 10 and 20, the phrase "such as" (lines 3 and 6) renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d). In the interest of compact prosecution, the limitations following the phrase "such as," and ending with a semicolon, subsequently are ignored.

Also, the term "a card" (line 7) in claim 10 is a relative term which renders the claim indefinite. The term "a card" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. In the interest of compact prosecution, this limitation subsequently is ignored.

Regarding claim 15, the claim recites the limitation "said entity" (lines 4 and 5). There is insufficient antecedent basis for this limitation in the claim.

Regarding claims 16-19 and 32-35, the claims recite the limitation "said entity" (line 2). There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-3, 8, 10, 21-23, 27, 36, 37, 39 and 40 are rejected under 35

U.S.C. 102(e) as being anticipated by Dulude et al., hereafter Dulude (US 6,310,966).

Regarding claim 1, Dulude discloses a person authentication system comprising:

an entity for executing person authentication (receiver station 42),

wherein said entity acquires a template from a person identification certificate storing template information (biometric certificate 68) including said template and generated by a third-party agency (registration authority 34) serving as a person identification certificate authority (col. 4, lines 12-65, and col. 6, lines 32-34), and

executes person authentication on the basis of the acquired template (col. 6, lines 58-65, and col. 7, lines 33-44).

Regarding claim 2, Dulude teaches all the limitations of claim 1, and further teaches that the person identification certificate authority includes a digital signature written by said person identification certificate authority (biometric certificate 68 contains digital signature 22; Fig. 2; col. 4, lines 55-65).

Regarding claim 3, Dulude teaches all the limitations of claim 1, and further teaches that

said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued (col. 5, lines 16-25),

acquires a template serving as person identification data of said person requesting the person identification certificate to be issued (col. 4, lines 25-32), and

generates a person identification certificate storing template information including said template (col. 4, lines 55-65).

Regarding claim 6, Dulude teaches all the limitations of claim 1, and further teaches that said entity is any one of a service provider which provides services to a user identified by said person identification certificate, a user device accessed by a user identified by said person identification certificate, and said person identification certificate authority (receiving section 42 is service provider; col. 8, lines 34-45, incorporating Vaeth, US 6035,402; see Vaeth, col. 6, lines 5-26).

Regarding claim 8, Dulude teaches all the limitations of claim 1, and further teaches that

said entity is a service provider which provides services to a user identified by said person identification certificate (receiving section 42 is service provider; col. 8, lines 34-45, incorporating Vaeth, US 6035,402; see Vaeth, col. 6, lines 5-26), and

that said service provider compares a template (registration biometric data 72), which is acquirable from the person identification certificate acquired from said person identification certificate authority (col. 4, lines 55-65, and col. 6, lines 32-34), with

sampling information provided by the user (transaction biometric data 46) and starts providing services with the user, provided that said template and said sampling information match with each other (col. 7, lines 33-67).

Regarding claim 10, Dulude teaches all the limitations of claim 1, and further teaches that said template (registration biometric data) is composed any one of: biometric information of a person; non-biometric information; any combination of two or more of said biometric information and said non-biometric information; and a combination of any of said information and a password (template composed of biometric information; col. 4, lines 26-32 and 55-57).

Regarding claims 21-23 and 27, these are a method version of the claimed system discussed above (claims 1-3 and 8, respectively), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also are anticipated.

Regarding claims 36 and 37, these are an information-processing-apparatus version of the claimed system discussed above (claims 1 and 2), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also are anticipated.

Regarding claim 39, Dulude teaches all the limitations of claim 1, and further teaches that

that said information processing apparatus compares a template (registration biometric data 72), which is acquirable from the person identification certificate acquired from said person identification certificate authority (col. 4, lines 55-65, and col. 6, lines

32-34), with sampling information provided by the user (transaction biometric data 46) and starts providing services with the user, provided that said template and said sampling information match with each other (col. 7, lines 33-67).

Regarding claim 40, this is a program-providing-medium version of the claimed system discussed above (claim 1), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such a claim also is anticipated.

8. **Claims 1, 9, 21, 24, 28, 36, 38 and 40 are rejected under 35 U.S.C. 102(e)** as being anticipated by Bianco et al., hereafter Bianco (US 6,256,737).

Regarding claim 1, Bianco discloses a person authentication system comprising:

an entity for executing person authentication (computer 208 containing biometric device object 722),

wherein said entity acquires a template from a person identification certificate storing template information (biometric template) including said template and generated by a third-party agency (biometric server 104) serving as a person identification certificate authority (col. 24, lines 21-31), and

executes person authentication on the basis of the acquired template (col. 24, lines 37-39).

Regarding claim 9, Bianco teaches all the limitations of claim 1, and further teaches

that said entity is a user device serving as a data processing apparatus including data accessible by a user identified by said person identification certificate (computer 208; col. 11, line 66, through col. 12, line 22), and

that said user device compares a template, which is acquirable from the person identification certificate acquired from said person identification certificate authority, with sampling information provided by the user (col. 24, lines 21-43, and col. 25, lines 31-50),

and said user device allows the user to start accessing said user device, provided that said template and said sampling information match with each other (col. 24, lines 40-56).

Regarding claims 21, 24 and 28, these are a method version of the claimed system discussed above (claims 1, 4 and 9, respectively), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also are anticipated.

Regarding claims 36 and 38, this is an information-processing-apparatus version of the claimed system discussed above (claims 1 and 4), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also are anticipated.

Regarding claim 40, this is a program-providing-medium version of the claimed system discussed above (claim 1), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such a claim also is anticipated.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. **Claims 5, 7, 25 and 26 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Dulude in view of Hughes ("Digital Envelopes and Signatures," InstantDoc #2698, WindowsITPro, September 1996).

Regarding claim 5, Duluth teaches all the limitations of claim 1, but does not explain the further limitation that said person identification certificate authority stores said template in said person identification certificate after encrypting said template.

However, Hughes teaches a method for securing the transmission of a message wherein both the encryption of the message and the digital certificate (signature) for the message sender are employed concurrently for the purpose of providing both privacy and authentication (page 3, paragraph 5).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Dulude with the teaching of Hughes such that said person identification certificate authority stores said template in said person identification certificate after encrypting said template, particularly where the biometric database 66 which stores the biometric certificate 68 is accessed over a network connection (col. 5, lines 33-44 and col. 6, lines 32-43). One would be

motivated to do so in order to ensure both privacy and authentication in transmission of the biometric certificate over a network.

Regarding claim 7, Duluth teaches all the limitations of claim 1, but does not explain the further limitation that, when transmitting said person identification certificate to said entity, said person identification certificate authority transmits a template which is stored in said person identification certificate, as an encrypted template which is decryptable only by said entity to which said person identification certificate is to be transmitted.

However, Hughes teaches a method for securing the transmission of a message wherein both the encryption of the message and the digital certificate (signature) for the message sender are employed concurrently for the purpose of providing both privacy and authentication (page 3, paragraph 5), and wherein the encrypted message is decryptable only by the entity to which the certificate is to be transmitted (page 2, paragraph 2).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Dulude with the teaching of Hughes such that, when transmitting said person identification certificate to said entity, said person identification certificate authority transmits a template which is stored in said person identification certificate, as an encrypted template which is decryptable only by said entity to which said person identification certificate is to be transmitted, particularly where the biometric database 66 which stores the biometric certificate 68 is accessed over a network connection (col. 5, lines 33-44 and col. 6, lines 32-43). One

would be motivated to do so in order to ensure both privacy and authentication in transmission of the biometric certificate over a network.

Regarding claims 25 and 26, this is a method version of the claimed system discussed above (claims 5 and 7), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also would have been obvious.

10. **Claims 4 and 11 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Bianco in view of Diffie et al., hereafter Diffie, ("Authentication and Authenticated Key Exchanges," Designs, Codes and Cryptography, Kluwer Academic Publishers, 1992).

Regarding claim 4, Bianco teaches all the limitations of claim 1, and further teaches that said person identification certificate authority transmits the person identification certificate to said entity (col. 24, lines 21-32).

Although Bianco teaches that the transmission of the certificate between said person identification certificate authority and said entity is encrypted using an asymmetric public key protocol (col. 55, lines 29-57, and col. 56, lines 52-65), Bianco does not explain that in the process of acquiring the person identification certificate from said person identification certificate authority, said entity performs mutual authentication between said entity and said person identification certificate authority, and said person identification certificate authority transmits the person identification certificate provided that said mutual authentication is successfully completed.

However, Diffie teaches a method of two-party mutual authentication wherein the parties exchange digital signatures (page 9, first paragraph) in addition to their public cryptographic keys for the purpose of enhancing security by assuring that each of the parties exchanging a public key is authentic and not an imposter (page 2, paragraph 3).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Bianco with the teaching of Diffie such that in the process of acquiring the person identification certificate from said person identification certificate authority, said entity performs mutual authentication between said entity and said person identification certificate authority, and said person identification certificate authority transmits the person identification certificate provided that said mutual authentication is successfully completed. One would be motivated to do so in order to enhance network security by assuring that each of the parties exchanging a public key is authentic and not an imposter.

Regarding claim 11, Bianco teaches all the limitations of claim 1, and further teaches

that said entity and said person identification certificate authority have an encryption processing unit, respectively, (col. 56, lines 58-65).

But Bianco does not explain that when data is transmitted between said entity and said person identification certificate authority, mutual authentication is performed, a data-transmitting party generates a digital signature and adds it to data to be transmitted, and a data-receiving party verifies the digital signature.

However, Diffie teaches a method of two-party mutual authentication wherein the parties exchange digital signatures (page 9, first paragraph) in addition to their public cryptographic keys for the purpose of enhancing security by assuring that each of the parties exchanging a public key is authentic and not an imposter (page 2, paragraph 3).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Bianco with the teaching of Diffie such that when data is transmitted between said entity and said person identification certificate authority, mutual authentication is performed, a data-transmitting party generates a digital signature and adds it to data to be transmitted, and a data-receiving party verifies the digital signature. One would be motivated to do so in order to enhance network security by assuring that each of the parties exchanging a public key is authentic and not an imposter.

11. Claims 12-14, 20 and 29-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yu et al. al., hereafter Yu (US 5,930,804), in view of Duluth.

Regarding claim 12, Yu discloses a person authentication system comprising:
a person identification certificate authority (authentication center 24 containing biometric server 42) which acquires a template (stored biometric data),

executes person authentication on the basis of said acquired template (col. 11, lines 5-13), and

issues a verification certificate, provided that said person authentication is successfully passed (col. 11, lines 66-67, and col. 12, lines 33-43).

But Yu does not explain that the person identification certificate authority acquires the template from a person identification certificate storing template information including said template.

However, Duluth teaches an authentication system wherein a template (registration biometric data 20) is stored within a person identification certificate (biometric certificate 68; Fig. 2; col. 4, lines 55-65; col. 5, lines 33-35) for the purpose of facilitating increased security and accuracy in the authentication of electronic transactions by binding the biometric identification of consumers with digital certificates (col. 3, lines 28-34).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Yu with the teaching of Duluth such that the person identification certificate authority acquires the template from a person identification certificate storing template information including said template. One would be motivated to do so in order to facilitate increased security and accuracy in the authentication of electronic transactions by binding the biometric identification of consumers with digital certificates.

Regarding claim 13, the modified invention of Yu and Duluth is relied upon as applied to claim 12, and Yu further teaches that the verification certificate issued by said person identification certificate authority includes a digital signature written by said person identification certificate authority (Yu, col. 12, lines 36-57).

Regarding claim 14, the modified invention of Yu and Duluth is relied upon as applied to claim 12, and Yu further teaches that

said person identification certificate authority acquires a template serving as person identification data of said person requesting the person identification certificate to be issued (col. 9, lines 54-63).

But Yu does not explicitly explain that said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued and that said person identification certificate authority generates a person identification certificate storing template information including said template.

However, Duluth teaches an authentication system wherein said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued (col. 5, lines 15-25) and wherein a person identification certificate authority (registration authority 34) generates a person identification certificate (biometric certificate 68) storing template information (registration biometric data 20) including said template (Fig. 2; col. 4, lines 55-65) for the purpose of facilitating increased security and accuracy in the authentication of electronic transactions by binding the biometric identification of consumers with digital certificates (col. 3, lines 28-34).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the modified invention of Yu and Duluth as applied to claim 12 with the further teaching of Duluth such that said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued and that said person identification certificate authority generates a person identification certificate storing template information

including said template. One would be motivated to do so in order to facilitate increased security and accuracy in the authentication of electronic transactions by binding the biometric identification of consumers with digital certificates.

Regarding claim 20, the modified invention of Yu and Duluth is relied upon as applied to claim 12, and Yu further teaches that said template is composed of any one of: biometric information of a person; non-biometric information; any combination of two or more of said biometric information and said non-biometric information; and a combination of any of said information and a password (biometric data; col. 9, lines 54-67, and col. 10, lines 61-67).

Regarding claims 29-31, this is a method version of the claimed system discussed above (claims 12-14), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also would have been obvious.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Cordery et al. (US 5,796,841) teaches a system for authentication of users for e-commerce involving digital certificates.


Deo et al. (US 5,721,781) teaches a system for mutual authentication of entities over a network by exchanging digital signatures.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JE


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100